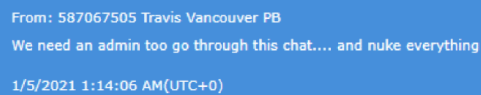


# THE PROUD BOYS' RELIANCE ON TELEGRAM DIDN'T SAVE THEM, BUT IT THWARTED PREVENTING THE ATTACK

At 8:06PM on January 4, 2021, shortly after the arrest of Enrique Tarrío, a Proud Boy named Travis instructed everyone on the Proud Boys' Ministry of Self Defense Telegram list to "nuke everything."



From: 587067505 Travis Vancouver PB  
We need an admin too go through this chat.... and nuke everything  
1/5/2021 1:14:06 AM(UTC+0)

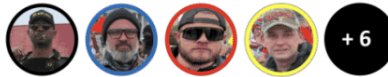
Because of the way Telegram persists on individual phones, it didn't work. Two years later, that text was introduced as evidence against the Proud Boys to show that already on January 4, they knew they had something to hide.

Four days later, on the Ministry of Self Defense list that had replaced the first one, Aaron of the Bloody East – a senior Proud Boy in Philadelphia – announced the arrest of Proud Boy Nicholas Ochs as he landed in Hawaii (the avatars for the Proud Boys were added for the trial exhibit; only the monikers and user numbers came from Telegram itself). The conversation immediately turned to deleting two channels used to organize the Proud Boys during January 6. But because Jeremy Bertino, who had set up the chat, had already left it, the men once again struggled to cover their tracks.



New MOSD

Jan. 8, 2021



Time	Name	Message
7:23:48 AM	Aaron Of The Bloody East 668358826	They got Nick
7:23:48 AM	Aaron Of The Bloody East 668358826	🔒Need this Echoed🔒  Our Journalist Nick Ochs has been arrested in Hawaii for covering the 'Stop the Steal' event in D.C.  <a href="https://parler.com/post/8a733e48cca94691b27b8484de5fb6e4">https://parler.com/post/8a733e48cca94691b27b8484de5fb6e4</a>
7:25:47 AM	Noble Beard The Immortal 1261651524	Fuck!!
10:31:08 AM	Johnny Blackbeard 759787552	Its probably time to clean up the chats from DC
10:31:19 AM	Johnny Blackbeard 759787552	We don't need the boots on the ground one
10:32:43 AM	Noble Beard The Immortal 1261651524	<i>I left it and I can't delete it. It wouldn't allow me to delete, for some reason.</i>
10:34:50 AM	Johnny Blackbeard 759787552	Its locked and there is no owner or admin. I've never seen that happen
10:35:08 AM	Noble Beard The Immortal 1261651524	Yeah me neither
10:47:44 AM	Aaron Of The Bloody East 668358826	I think if the owner leaves the chat it becomes a zombie chat with no admins

Organizing on Telegram did not prevent the government from prosecuting the Proud Boys for their roles in January 6. On the contrary, those chats – complete with their boisterous efforts to delete them after every arrest – were a central part of the evidence used to prosecute Enrique Tarrio, Joe Biggs, and Ethan Nordean on sedition charges, with help from Bertino, who had flipped and who continues to cooperate in the investigation.

It started no later than Nordean’s own arrest on February 3, 2021, when Nordean’s spouse provided the FBI with the passcode to his phone, where many of these texts were still available. It continued as the FBI acquired one after another of the Proud Boys’ phones (one of the only known exceptions was Joe Biggs, whose phone the FBI never got).

A letter to Zach Rehl’s attorney from 2022 gives a sense of how the FBI had to exploit as many phones as they could, one after another, because

the set of texts still available on any individual's phone varied. Some people, like Nordean, were successful at deleting their voice notes and other attachments. Others didn't even try.

Altogether, DOJ relied on at least 11 separate lists, as well as a slew of individual Telegram texts (as well as a number of Parler texts), at trial. In that sense, the investigation of the Proud Boys was little different than that of the Oath Keepers, who used Signal rather than Telegram for that kind of organization.

That's important background to news of the French arrest of Pavel Durov on charges implicating (at least) child sexual exploitation, terrorism, cybersecurity, fraud, and organized crime. Authorities can still prosecute people who use Telegram to plan and organize their crimes.

But there are impediments. The cops took Tarrío's phone when they arrested him – with those damning Telegram threads still on it – two days *before* the Proud Boys would lead a mob that attacked the Capitol. But it took over a year before they cracked the encryption on his phone, exploited it, and did a privilege review. Even after seizing Tarrío's phone, then, prosecutors couldn't *prevent* January 6 having decided that Tarrío posed a risk to the certification of the vote only days before the attack.

It might have been different if the Proud Boys had been considered a terrorist group (which it still is not, in significant part because of an asymmetry in US law regarding domestic and foreign extremist groups). Contrary to what a lot of coverage is reporting, the vast majority of Telegram usage is not encrypted. As far as I'm aware, none of the texts introduced at the Proud Boy trials were protected by Telegram's hard to use encryption, not even the private texts in which Tarrío told one after another of his girlfriends of his imminent arrest.

But the encryption itself would not have saved

him. On December 18, 2020 DC cop Shane Lamond did turn on Telegram's encryption in texts he was exchanging with Tarrío, warning him about both the investigation into his role in burning a BLM flag (the crime for which Tarrío would be arrested on January 4), as well as observations about public Proud Boys statements in advance of January 6.


To contact Tarrío, the Defendant used a chat on Telegram with the highest level of encryption available. The Defendant then asked Tarrío if he had called in the anonymous tip. Tarrío responded "I did more than that. It's on my social media." The Defendant told Tarrío "I'm curious to see what happens too. I will check with our CID [Criminal Investigations Division] people if they have you on video."

But those were still available on the phones after the fact.

Even after Lamond and Tarrío set Telegram to auto-delete messages, Telegram's functionality didn't entirely save them.

On December 22, 2020, approximately two minutes after Tarrío sent the Defendant a screenshot of a message he received from an MPD detective assigned to the BLM Banner Burning Investigation through Telegram, the Defendant changed the settings of his encrypted chat with Tarrío on Telegram so that future messages would delete 5 seconds after the recipient opened them.

Some of their auto-delete texts were reconstructed, especially those sent after Tarrío's pre-trial release on the DC case.

From	To	Content	Attachment #1 Preview
Enrique Tarrío <581632416>	Shane Lamond <869476955>	<MessageID 28> Enrique set the self-destruct timer to 30 seconds	
Shane Lamond <869476955>	Enrique Tarrío <581632416>	<MessageID 34> <Self-Destruct Timer: 30 seconds> Hey brother, are your guys planning to come to DC on March 4th?	
Shane Lamond <869476955>	Enrique Tarrío <581632416>	<MessageID 35> <Self-Destruct Timer: 30 seconds> Bump	
Shane Lamond <869476955>	Enrique Tarrío <581632416>	<MessageID 36> <Self-Destruct Timer: 30 seconds> <a href="https://www.reuters.com/article/us-usa-proudboys-leader-idUSKBN29W1PE">https://www.reuters.com/article/us-usa-proudboys-leader-idUSKBN29W1PE</a>	

And after Lamond called Tarrío using Telegram to warn him about the warrant for his arrest, Tarrío went to the Ministry of Self Defense thread – the same one the Proud Boys failed to delete after his arrest – and told them that his contact had just warned him of the arrest. There are texts between Lamond and Tarrío, especially from January 1 and 4, which were lost to law enforcement. But enough of their texts were preserved to substantiate obstruction charges on which Lamond will go to trial in October.

The encryption didn't save Shane Lamond. It would probably do little for intelligence targets either – in part because the encryption may not be all that great, but also because a determined spook is going to get texts via the phones, just like the FBI did with Lamond. France certainly has the intelligence capabilities to defeat Telegram's encryption, as does the US, both of which would be happy to share with Ukraine.

Rather, one of France's reported complaints is that Telegram won't cooperate with law enforcement requests. Even though all these threads via which the Proud Boys planned January 6 and the texts sent between the allegedly corrupt cop Lamond and Tarrío before December 18 were likely readily available on Telegram's servers, even if the FBI had asked after Tarrío's arrest, Telegram wouldn't have provided them, at least not without a whole bunch of squawking. That also means that Telegram wouldn't provide a whole bunch of other information that proves useful to solving crimes. In the Proud Boys case, because prosecutors couldn't get metadata directly from Telegram, it likely required cooperating witnesses like Bertino to attribute the handles used by some of the Proud Boys to specific users

(at the time, Signal did not yet have this capability, so investigators could more easily match phone numbers to users).

By comparison, prosecutors could and did serve preservation orders on Google and Facebook, which preserved a lot but by no means all relevant content, even as individual users were trying to cover their tracks just like the Proud Boys were. In response to legal process, those platforms, as well as Twitter and others (but not Signal, which doesn't keep most of this data), provided user data, address, credit card data, and access times.

But it's the issue of *prevention* for which Telegram poses the biggest concern. Telegram is the platform of choice for extremists of all ideologies, both for broadcast messaging and for more discreet threads like the ones the Proud Boys used. And in quick moving situations, like the extremist mobilization in the wake of the Southport stabbing in the UK, Telegram channels can grow to include tens of thousands before they're even discovered. While Telegram took the rare step, in that case, of shutting down the most violent channels tied to British riots, it left many of them up.

It's still too early to know the scope of the French investigation, beyond that it implicates both non-cooperation and slow moderation. It's a complaint both that Telegram won't provide information to solve crimes already committed and won't take steps to prevent them from happening.

Two of the most important questions are whether Durov derives a material benefit from letting crime and extremism flourish on Telegram. Another is whether Durov gives the Russian government preferential access to all the channels that are otherwise difficult to access. This post provides a sense of the degree to which Durov's likely cooperative relationship with Russia conflicts with his public claims of animosity.

There are a lot of people claiming that France is targeting Durov because Telegram is an encrypted messaging platform. While that may be a factor, the far more important one is that Telegram allows crime to flourish on its platform, and until he arrived in France, where his French citizenship will actually help France thwart any Russian attempts to help him, he was protected by regimes that similarly preferred to let certain kinds of noxious content to thrive.

Update: The French have released the possible charges. There is one charge of refusing to cooperate in criminal investigations.

They include six charges of “complicité,” what I guess is the US equivalent to aid and abetting:

- Illegal transactions for organized crime
- Child sexual abuse material
- Organized dissemination of CSAM
- Narcotics sales
- Hacking tools
- Organized fraud

Then there are three crimes pertaining to the provision of encryption and importation of encryption without declaration.

The most interesting – and the ones that might make this prosecution akin to those of people like Ross Ulbricht – are:

- Association with criminals with the intent to commit crimes punishable by 5 years
- Money laundering

I noted above that one of the big questions is whether Durov derives a material benefit from letting crime flourish on Telegram. If he’s personally involved in money laundering, he may.

Note, none of the crimes suggest an unlawful

relationship with Russia (though some of those encryption crimes may originally have been targeted towards spooks).